Solution Spotlight

BlueVoyant MXDR for Microsoft
(Managed Extended Detection and Response)
Microsoft SIEM plus XDR Implementation and Management

A cloud-native, fully-integrated security solution helps companies operate safely in today's interconnected world. To bring this vision to life and help our clients achieve their business and security outcomes, BlueVoyant has partnered with Microsoft. In addition to making a significant investment in people, process, and technology, BlueVoyant offers clients an end-to-end portfolio of consulting, implementation, and managed security services, all powered by Microsoft's security technologies and designed to expand on your existing Microsoft security tools investment. We call this automation portfolio and 24×7 human security services BlueVoyant MXDR for Microsoft SIEM plus XDR.

MXDR for Microsoft SIEM plus XDR provides a complete portfolio of Microsoft security-focused services, including a customized deployment of Microsoft security tools, ongoing management and maintenance, as well as 24×7 MXDR, protecting you from cyber threats and providing continuous security posture improvement.

Consulting and Implementation

With MXDR for Microsoft, you don't need to be an expert to take your security and compliance posture to the next level. Our Accelerator services are focused consulting engagements designed to get you up and running quickly and maximize your investment in Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud security technologies. BlueVoyant performs a detailed analysis of your environment(s) and provides actionable security insights, leveraging the BlueVoyant catalog of prebuilt playbooks and alert rules.

What's included:

- A detailed assessment of your risks
- Guidance on how to best use Microsoft-powered solutions and deployments
- Configuration assistance to meet your unique requirements

Microsoft 365 Defender Accelerator

Microsoft 365 Defender Accelerator Defender for Endpoint; Defender for Identity; Defender for Office 365; Cloud App Security (MCAS)

- Infrastructure setup
- Configuration
- Integration with SIEM
- Policy tuning
- Integration with MXDR monitoring
- Security controls deployment

Solution Features

Microsoft Sentinel Accelerator

- Infrastructure setup
- Log source ingestion
- Alert and SOAR configuration
- Knowledge transfer
- Initial alert tuning and optimization
- Integration with MXDR monitoring
- Incident response playbook creation
- Security controls deployment

BlueVoyant

BlueVoyant MXDR for Microsoft SIEM plus XDR

MXDR for Microsoft activates 24×7 monitoring, detection, investigation, hunting, and response capabilities to augment Microsoft security tools and to work alongside customer security tools and personnel.

- **Microsoft Sentinel**
  Monitoring and investigations of infrastructure and log alerts surfaced via Microsoft Sentinel.
- **Microsoft 365 Defender**
  Monitoring, investigations, and remediation for Microsoft 365 content, with the Microsoft 365 security signals.
- **Defender for Cloud**
  Monitoring with investigation support for cloud workloads.

Solution Features

24×7 MXDR for Microsoft

- Alert triaging and investigation
- Unlimited remote incident response
- Threat eradication within Microsoft 365 Defender
- Threat intelligence
- Environment security health monitoring
- Log source collection, optimization
- Threat hunting
- Access to BlueVoyant library of 900-plus customized alert rules, hundreds of data connectors, and playbook automations
- Concierge Support included
- Escalations and notification as appropriate

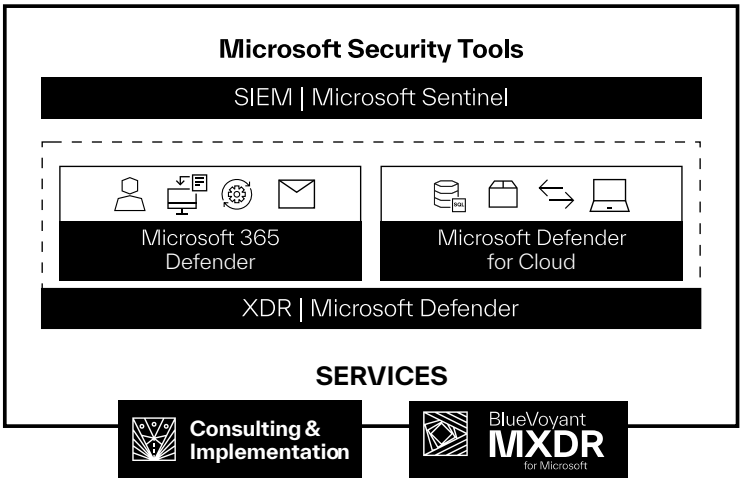
BlueVoyant MXDR for Microsoft is a powerful solution that can incorporate security logs from the entire Microsoft SIEM plus XDR security toolset as well as many thirdparty technologies.

Rather than sending BlueVoyant your logs and receiving alerts back, our security experts operate inside your environment. Watch in real time as they enrich investigations, raise alerts and close incidents, directly within your Microsoft Sentinel environment.

Benefits

- Reduce the level of risk faced by your organization
- Have more time to focus on other strategic activities.
- Integrate with your ticketing system
- Maximize your Microsoft investments
- Gain total value from M365 E3, E5, A5, G5, EMS, or Business Premium License.
- Consolidate cyber security into one solution
- Regulatory reports help you remain compliant.
- Gain maximum cost benefits by using only the logs that matter
- Your Technical Customer Success Manager will serve as your primary point of contact with BlueVoyant and collaborate with both you and our internal teams.
- As part of the MXDR for Microsoft service, you will have access to the
- BlueVoyant Security Operations Center 24×7. Every time you call, you'll speak to a human who will immediately address your questions.

MDR for Microsoft supports the entire Microsoft security suite



BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based cloud-native platform by continuously monitoring your network, endpoints, attack surface, and supply chain, as well as the clear, deep, and dark web for threats. The full-spectrum cyber defense platform illuminates, validates, and quickly remediates threats to protect your enterprise. BlueVoyant leverages both machine-learning-driven automation and human-led expertise to deliver industry-leading cybersecurity to more than 900 clients across the globe.

BlueVoyant

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**